

¿Odias las contraseñas?

Entra en el futuro gracias a la biometría.

Las contraseñas son el eslabón más débil a la hora de proteger las cuentas digitales. Los estafadores se apoderan de las cuentas utilizando vectores de ataque bien conocidos, como el phishing, el man-in-the-middle, la fuerza bruta y los ataques de relleno de credenciales, así como técnicas emergentes que aprovechan la IA.

Una herramienta de descifrado de contraseñas basada en inteligencia artificial (IA) llamada **PassGAN** ha sido probada recientemente con más de 15 millones de contraseñas.

Descifró el 51% en menos de un minuto

y el 81% en menos de un mes.¹



Por desgracia, la economía digital actual no ha hecho sino agravar el problema.



Hoy en día **una persona tiene una media de aproximadamente**

100 contraseñas que recordar y gestionar.²

El resultado es que la mayoría de la gente acaba reutilizando la misma contraseña o contraseñas similares en docenas de sitios y aplicaciones.

73%

de las personas **duplican sus contraseñas** tanto en sus cuentas personales como en las del trabajo.³

Y el **43% ha compartido** al menos una contraseña con un colega, amigo o familiar.⁴



Esto supone GRANDES pérdidas para las empresas, ya que el **90% de las filtraciones de datos están causadas por credenciales comprometidas.**⁵

En 2022, el **coste medio de una violación de datos**

alcanzó la cifra récord de

\$4.35 millones.

¡Es hora de cambiar!

La **autenticación biométrica** ofrece una forma fiable de autenticar con confianza a los clientes sin depender de las contraseñas.



Un estudio del Ponemon Institute mostró que el **56%**

de los profesionales de IT cree que eliminar las contraseñas mejoraría la seguridad de su organización, y el

65% cree que la biometría aumentaría la seguridad.⁶



De hecho, el

92%

de las organizaciones creen que **ofrecer una experiencia sin contraseña** a los usuarios finales es el futuro de su empresa.⁷

RECONOCIMIENTO FACIAL

ESCANEANDO... 70%

Lo **mejor de la biometría** es que es única para cada persona. Esto significa que no puede ser compartida, robada u olvidada, lo que hace de la biometría una defensa increíblemente fuerte contra el fraude.

Las pruebas de IDR&D han demostrado

que la **combinación de la biometría facial y vocal**, junto con la detección de vida, es

100X

más eficaz para prevenir el fraude que los métodos de autenticación tradicionales.⁸

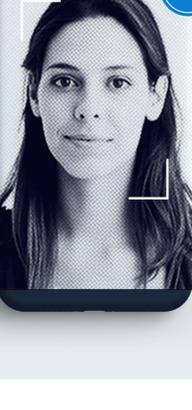
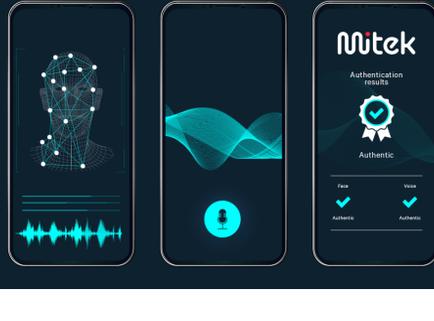
La **biometría no sólo ofrece un método de autenticación más seguro**, sino que también proporciona una mejor experiencia de usuario.



El **60%** de los consumidores afirma haber **abandonado una transacción comercial debido a su frustración con el proceso de autenticación**, y el

81%

prefiere interactuar con empresas que verifiquen su identidad de forma "sencilla, rápida y segura."⁹



MiPass de Mitek puede confirmar la identidad de tus clientes en cuestión de segundos utilizando biometría multimodal para **proReducir** la fricción con el cliente y los costes del servicio de asistencia de IT, y protegerás tu negocio eliminando el vector de ataque más común para los estafadores.

Visita <https://www.miteksystems.com/es/autenticacion-biometrica> para saber cómo podemos ayudarte a aprovechar la autenticación biométrica multimodal en tu organización.

Contacta con nosotros

Fuentes:
 1 <https://thehustle.co/ai-roundup-guessing-passwords--conjuring-images-out-of-peoples--minds--and--writing-fortune-cookies/>
 2 <https://www.zipgia.com/advice/password-statistics/>
 3 <https://www.enzoic.com/blog/8-stats-on-password-reuse/>
 4 <https://cybersecurity.asee.co/blog/password-statistics-that-will-change-your-attitude/>
 5 <https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf>
 6 <https://mms.businesswire.com/media/20200219005336/en/773763/5/191522-Ponemon-Infographic-2020-final-1.jpg?download=1>
 7 <https://www.securitymagazine.com/articles/93522-of-businesses-believe-going-passwordless-is-the-future>
 8 <https://www.idrnd.ai/5-reasons-to-make-biometrics-part-of-multi-factor-authentication/>
 9 <https://www.biometricupdate.com/202110/consumers-prefer-biometrics-to-passwords-think-less-of-brands-with-bad-authentication>